基于多碱基组合映射编码和 DNA 计算的一次一密算法 *

彭维平，程丹华，宋　成

(河南理工大学计算机科学与技术学院，河南省焦作市 454000)

摘　要：为增强密码方案安全性，利用多碱基组合映射编码，采用模拟 DNA 生物操作的方式，提出了一种一次一密加解密方案。方案主要采用分段加密的机制，利用多碱基组合映射编码规则编码明文信息，通过 Logistic 逻辑映射系统生成随机数构造一次一密密钥本，为每一个明文段选择不同的密钥。加解密算法运用 DNA 碱基运算规则，并将部分参数和最终密文经过处理后通过安全信道传送给解密方。对图像的仿真和安全性的分析表明，密钥本的制作基于混沌映射和多碱基 DNA 编码规则两层操作，密钥空间足够大，并且攻击者在密文图像中得不到任何有用的统计数据，另外，随着需要加密的明文数据量增加，攻击者完全破解所需计算的密钥空间量呈指数级增长，增强了算法安全性。

关键词：DNA 密码；Logistic 映射；多碱基组合映射；一次一密密钥本；图像加密

中图分类号：TP309.7　　doi: 10.3969/j.issn.1001-3695.2018.01.0100

One-time-pad encryption scheme based on multibase combination mapping encoding and DNA computing

Peng Weiping, Cheng Danhua, Song Cheng

(*School of Computer Sciences & Technology Henan Polytechnic University*, *Jiaozuo Henan* 454000, *China*)

Abstract: In order to enhance the security of cryptographic scheme, using the multibase combination mapping encoding and the way of simulating the biological operation, a one-time-pad encryption scheme was proposed. The scheme mainly adopted the mechanism of segmentation encryption. The plaintext information was transformed into the DNA sequence by the multibase combination mapping encoding. The Logistic Logic Mapping System generated random numbers to construct a one-time-pad codebook and selected different key for each plaintext segment. The encryption/decryption algorithm used the DNA base algorithm and transmitted some of the parameters and the final ciphertext to the decryption side through a secure channel. Through the analysis of the simulation and security of the image emulation, it is shown that the production of the codebook is based on the two-level operation: the chaos mapping and the multibase combination mapping encoding, the key space is large enough, and the attacker can not obtain any useful statistical date in the ciphertext image. Moreover, with the increase of the plaintext data, the amount of key space required for the attacker to crack is exponentially increasing, which improves the security of the algorithm.

Key words: DNA cryptography; Logistic logic mapping; the multibase combination mapping encoding; one-time codebook; image encryption

0　引言

DNA 编码继承了遗传分子强大的并行计算能力、能耗低和高信息密度等特性[1]，使得 DNA 计算[2-6]和 DNA 密码在大量并行数据加密的应用中具有独特优势，也取得了一些成果，但其加密技术还很不成熟，还有很多亟需解决的问题，比如编码过程太复杂、生物实验失误率高、实验成本太高等。事实上，在 DNA 生物实验中因为操作环节多且错误会逐渐累积，所以要求实验操作的每个步骤都具备很高的成功率，否则得到的结果可能与准确值差别很大。当前，在 DNA 密码算法设计方面相对可行的方法是基于 DNA 计算的一些生物学特性，采用模拟 DNA 生物操作的方式，通过执行伪 DNA 计算的操作来实现信息加密[7]。2012 年，文献[8]利用设计的 DNA 组件，将接收到的语音信息转换成文本形式，再将该文本利用 DNA 编码转换成 DNA 序列的形式进行传送。文中设计使用的 DNA 编码规则为四个碱基组合对应英文字母、数字和特殊符号，密码本大小为 98，由于四个碱基组合的种类有 4^4 种，则其密钥空间仅为

收稿日期：2018-01-30；**修回日期：**2018-03-19　　**基金项目：**河南省科技攻关项目（182102110333）；河南理工大学博士基金项目（B2012-050）

作者简介：彭维平（1979-），男，湖北天门人，副教授，博士，主要研究方向为信息安全、DNA 密码学、物联网安全及应用（pwp9999@hpu.edu.cn）；程丹华（1991-），女，硕士研究生，主要研究方向为信息安全、DNA 密码；宋成（1980-），男，河南信阳人，讲师，博士，主要研究方向为信息安全、密码学、可信计算等.

C_{256}^{98}，在了解组件工作原理的情况下，利用穷举攻击密文信息很容易被破解得到明文。2014 年，文献[9]提出随机生成一次一密密钥本加解密的方案，通过 PCR 技术进行密钥分配，利用电子计算机异或运算进行加解密操作，信息转换采用三联体编码的方式，编码由三个碱基组成的组合与字母、数字和符号对应关系组成，分析可得其对应关系只有 C_{64}^{40} 种，所提供的编码安全性相对较低。2015 年，文献[10]提出一种改进的基于 DNA 编码和混沌映射的图像加密方法，利用 DNA 加法、DNA 减法和 DNA 补充方法三种算法对明文图像对应的 DNA 序列矩阵进行操作，补充了已有算法[11]的不可逆性的缺点。但是，从编码安全考虑，该算法使用的 DNA 编码规则为传统的单碱基与双比特二进制的对应关系，又考虑其互补特性，即只有 8 种编码选择方式，算法所提供的编码安全性是远远不够的。2016 年，文献[12]提出一种对称密钥密码方案，首先明文根据 ASCII 和传统的互补性 DNA 编码规则转换成 DNA 序列，将该序列 4 个一组根据随机密钥本找到相应最终的十进制密文。文中关键步骤在于随机密钥本的生成，该密钥本由四个碱基组合与 1~256 数字的对应关系组成，其密钥空间为 256!，但生成过程中需要排除较多具有相同对应关系的选择，因而实际可用的对应关系远远小于 256!。综合上述文献方案中明文转换和密钥本的构造均仅利用简单的字符和 DNA 碱基组合的对应关系，所得密钥空间均为一固定值，跟明文的长度等没有关系。

相比较以上基于 DNA 编码的密码方案，本文方案利用两种 DNA 碱基编码规则分别处理明文信息、制作密钥本和密文传输，针对不同数据选择不同的 DNA 编码规则，以增强算法编码安全性，并且，利用传统的一维 Logistic 混沌映射对初始值的随机性和敏感性等固有特性制作一次一密密钥本，通过代入初始参数产生多对参数，根据设计的算法规则和编码规则经过转换添加引物信息后得到相应的单链 DNA 序列集合，即为密钥本。为增强安全性，加密完成后将密钥本制作的初始参数、挑选密钥的引物对和密文进行信息处理转化为可在安全通信信道传输的二进制序列传送给解密方，解密方收到密文，首先经过数据处理得到初始参数等，根据密钥本制作规则生成密钥本，再利用和加密相同的算法解密密文。最后，本文以图像为仿真对象，描述了算法的整个过程，分析表明本方案密钥空间与明文长度相关，并从密钥敏感度、灰度直方图、信息熵等方面分析了本方案的可行性和安全性。

1　算法基础

1.1　相关参数

本文所用的参数如表 1 所示。

表 1　相关参数定义

参数	定义
DNA 编码规则	$R(N_1 \sim N_4)$
Logistic 混沌映射初始参数	(g_1, μ_1)
阈值函数	$F(x)$
明文二进制长度	n
明文分段长度	l
明文分段段数	S
图像矩阵	$M \times N$
密钥本大小	K
单个密钥长度	m
信息熵	$H(x)$

1.2　DNA 编码

DNA 由 A（腺嘌呤脱氧核苷酸），T（胸腺嘧啶脱氧核苷酸），C（胞嘧啶脱氧核苷酸）和 G（鸟嘌呤脱氧核苷酸）四个脱氧核苷酸组成，其中 A、T 和 C、G 分别两两互补。为了提高方案的安全性，本文分别对明文转换和密文传输使用不同的编码规则，定义如下所示。

编码规则 1　单碱基映射双比特二进制编码[13]：将 DNA 碱基 A,T,C,G 分别表示双比特二进制值 00,01,10,11。

很显然，此对应方式有 $4!=24$ 种，考虑 DNA 碱基之间的互补特性，实际可用的编码有 8 种，如表 2 所示。本文后续方案中密文等转换传输时采用的编码规则均选自于表 2。

表 2 DNA 编码 I

1	2	3	4	5	6	7	8
00-A	00-A	00-C	00-C	00-G	00-G	00-T	00-T
01-C	01-G	01-A	01-T	01-A	01-T	01-C	01-G
10-G	10-C	10-T	10-A	10-T	10-A	10-G	10-C
11-T	11-T	11-G	11-G	11-C	11-C	11-A	11-A

编码规则 2　多碱基组合映射双比特二进制编码：a 个碱基组成的组合分别对应双比特二进制 00,01,10,11，在碱基 A,T,C,G 中任选 a 个碱基进行组合，则共有 4^a 种组合方式。

很显然，当 $a=1$ 时，此规则等价于上述编码 I。

假设 $a=4$，则 4 个碱基共有 4^4=256 种组合方式，双比特二进制值随机对应 4 种不同的碱基组合方式。本文后续明文二进制串向明文 DNA 序列转化时运用此编码规则。

1.3　DNA 碱基运算

碱基之间除了 DNA 生物特性方面的反应之外，有专家和学者提出了构造算术或逻辑运算的方法，比如加法、减法运算，与、或、非和异或等逻辑运算。为遵循碱基之间互补特性和便于进行加解密运算，本文 DNA 碱基运算只采用异或运算操作。根据 1.2 节中的编码规则 I，有 8 种不同的 DNA 编码方案，每一种编码方案对应相应的碱基运算结果。因而，可构造出 8 种不同的碱基运算表。例如，选用表 1 中的编码规则 I（$[A=00, T=11, C=01, G=10]$），按照传统异或算法可得 DNA 碱基之间的运算表如表 3 所示。

表 3 DNA 碱基运算表

运算结果	A	T	C	G
A	A	T	C	G
T	T	A	G	C
C	C	G	A	T

G	G	C	T	A

1.4 随机数生成

基于一维 Logistic 混沌映射产生伪随机序列，并通过阈值函数可得到随机性很强的二进制序列，其数学定义如下所示，每个随机序列均由初始参数 (g_1,μ_1)，$g_1\in(0,1),\mu_1\geq 3.569946$ 和阈值来确定，其中 $x_1=g_1$。

$$x_{i+1}=\mu_j x_i(1-x_i),\mu_j\in[0,4],x_i\in(0,1) \tag{1}$$

$$F(x)=\begin{cases}0, & 0<x_i\leq 0.7\\ 1, & 0.7<x_i<1\end{cases} \tag{2}$$

本文采用参数派生的方法，通过一组初始参数来产生多组参数，派生计算如下公式所示：

$$\mu_i=\mu_1+10^{-w}\times(i-1)\ \ ,w\text{为正整数且}w\geq 3 \tag{3}$$

$$g_i=\mu_i g_{i-1}(1-g_{i-1}),\quad g_i\in(0,1),\mu_1\in[3.569946,4] \tag{4}$$

2 密码本构造

一次一密密钥本用于密码算法具有更高的加密强度，其所需密钥的长度取决于待加密明文的长度。为便于密钥的生成和管理，本文采用分段加密的方式，将明文对应的二进制信息进行分段加密操作，加解密所用的单个密钥长度不小于明文分段长度。每段明文可随机选择密钥本中不完全相同的任意一条密钥段进行加解密。

2.1 分段规则

本文将明文数据归纳为文本信息和非文本信息两大类，非文本信息以图像信息为例。针对两种不同的数据类型，采用不同的分段方法，规则如下：

1)文本信息分段

文本信息首先转换为二进制，依据分段长度，即可计算出分段数。假设明文信息对应的明文二进制长度为 n，定义分段长度为 l、分段数为 S。

$$S=\lceil n/l\rceil \tag{5}$$

其中:第 S 段长度若小于分段长度 l，采用“0”填充方式补齐。

2) 图像信息分段

若加密的明文信息是图像数据，首先原始图像经过转化得到一个 $M\times N$ 的二进制矩阵，则默认原始图像对应的二进制矩阵的每一行为一段，矩阵的行数即为分段总数，即 $S=M$。

2.2 密钥生成算法

通过以上分析，设定密码本大小为 K，则 $K>S$。密钥产生及构造密码本算法如下：

a)设定混沌映射初始值 $(g_1,\mu_1),g_1\in(0,1),\mu_1\geq 3.569946$。将初始值 (g_1,μ_1) 代入式(3)(4)得到初始值在内共 K 对参数 $(g_i,\mu_i),g_i\in(0,1),\mu_i\geq 3.569946,i\in[1,K]$。

b)将 a)得到的 K 对参数 (g_i,μ_i) 均代入 Logistic 混沌式(1)中生成 K 个随机数序列 $\{\{(x_i)_1\},\{(x_i)_2\},\ldots\{(x_i)_k\}\}$，经过阈值函数式(2)判断得到 K 个二进制序列串 $\{\{(b_i)_1\},\{(b_i)_2\},\ldots\{(b_i)_k\}\}$。

c）依次从 b)中生成的 K 个二进制串中截取不完全相同的长度为 m 的 K 条二进制序列 $\{\{(b_i,b_{i+1},\ldots b_{i+m-1})_1\},\{(b_i,b_{i+1},\ldots b_{i+m-1})_2\},\ldots\{(b_i,b_{i+1},\ldots b_{i+m-1})_k\}\}$。$m$ 的取值依据 2.1 节中对明文分段大小来确定，若加密数据为明文信息为文本信息，则 $m=l$；若为图像信息，则 $m=N$。

d)根据 1.2 中的编码规则 2，从 N_4 种对应方式中选择 K 种不完全相同的方式对截取出的 K 条二进制序列进行 DNA 转换，得到 K 条 DNA 单链序列 $\{\{D_1'\},\{D_2'\},\ldots\{D_K'\}\}$。

e)分别对 K 条 DNA 单链序列前后随机添加长为 10bp 的引物对 $\{(q_1,q_1'),(q_2,q_2'),\ldots(q_K,q_K')\}$。

此 K 条 DNA 单链构造的集合即为加解密的密钥本。约束条件：

K 条 DNA 单链必须符合以下条件：a）任意两条单链的引物对不完全相同；b）任意两条单链的密钥序列不完全相同。

3 加/解密算法设计

3.1 算法初始化

a)依据明文信息类别按照 2.1 节所述规则，计算得到分段参数 S，确定密钥本大小 K；

b)设定初始参数 (g_1,μ_1)、w、引物对信息 $\{(q_1,q_1'),(q_2,q_2'),\ldots(q_K,q_K')\}$、编码规则 I 中的 R_1 以及编码规则 II 中的 R_2 和 R_3。

c)以上参数通过安全信道传送给解密方。

3.2 加密算法

初始化完成后，依据初始参数，构造密码本，在密码本中选择 S 对引物对应的密钥作为加密密钥，并和明文段按照碱基运算规则进行加密操作。具体加密步骤如下：

a)根据 R_2 将明文二进制段转化为对应的明文 DNA 序列段 $\{\{D_1\},\{D_2\},\ldots,\{D_{S-1}\},\{D_S\}\}$；

b)利用共享参数 w、初始参数 (g_1,μ_1)、编码规则 R_3 以及全部引物对 $\{(q_1,q_1'),(q_2,q_2'),\ldots(q_K,q_K')\}$ 按照 2.2 节密钥本生成算法制作密钥本；

c)在引物对集合 $\{(q_1,q_1'),(q_2,q_2'),\ldots(q_K,q_K')\}$ 中随机挑选 S 对引物 $\{(q_i,q_i'),\ldots(q_S,q_S')\}$，从密钥本中对应挑选出 S 个密钥 $\{\{D_i'\},\ldots,\{D_S'\}\}$；

d)按照 1.3 节中 DNA 碱基运算规则对每段明文 DNA 序列 $\{\{D_1\},\{D_2\},\ldots,\{D_{S-1}\},\{D_S\}\}$ 和对应的密钥 $\{\{D_i'\},\ldots,\{D_S'\}\}$ 按顺序进行加密操作，得到密文 DNA 序列 $\{\{C_1\},\{C_2\},\ldots,\{C_{S-1}\},\{C_S\}\}$；

e)将引物对 $\{(q_i,q_i'),\ldots(q_S,q_S')\}$ 以及密文 DNA 序列 $\{\{C_1\},\{C_2\},\ldots,\{C_{S-1}\},\{C_S\}\}$ 按照 R_1 转化成适合通信信道传输的二进制编码发送给接收者。

3.3 解密算法

解密方得到密文信息后，首先根据共享参数制作密钥本，然后利用密文信息中的引物对信息选择密钥和密文进行解密。具体解密步骤如下：

a)根据初始参数 (g_1,μ_1) 按照密钥本生成规则和 R_3 生成 DNA 序列，并按顺序添加共享的全部引物对信息 $\{(q_1,q_1'),(q_2,q_2'),\ldots(q_K,q_K')\}$ 得到密钥本；

b)将密文二进制编码根据 R_1 还原得到引物对信息 $\{(q_i,q_i'),\ldots(q_S,q_S')\}$ 和原始密文 DNA 序列 $\{\{C_1\},\{C_2\},\ldots,\{C_{S-1}\},\{C_S\}\}$；

c)根据密文中引物对信息 $\{(q_i,q_i'),\ldots(q_S,q_S')\}$ 在密钥本中找到对应的密钥 DNA 序列 $\{\{D_i'\},\ldots,\{D_S'\}\}$；

d)密钥 DNA 序列 $\{\{D_i'\},\ldots,\{D_S'\}\}$ 和原始密文 DNA 序列 $\{\{C_1\},\{C_2\},\ldots,\{C_{S-1}\},\{C_S\}\}$ 依据 DNA 碱基运算规则进行操作得到明文 DNA 序列；

e)利用加密时操作明文信息的编码规则 R_2 还原明文 DNA 序列得到原始明文信息。

4 实验仿真

本文选择灰色图像作为仿真对象。明文图像可转化成每一个像素为 0~255 的二维矩阵。按照上述加解密流程，将明文图像的每一行作为一个明文段进行加密操作，为了达到更好的加密效果，在实施加密算法之后对图像进行 Arnold 置乱处理。以 Lena 图像为例，其大小为 256×256，原图经过转化得到一个大小为 256×2048 的二进制灰度值矩阵，将矩阵的每一行作为一段进行加密，即 S=256，$K>S$=256，设置密钥大小 $K=320$。首先，设定 Logistic 混沌映射初始值为 $g_1=0.504, \mu_1=3.68$，参数 $w=3$，初始值带入公式(3)和(4)，顺序选择 320 对参数 (g_i, μ_i) 带入公式(1)和(2)，对生成的每条随机二进制串从第 100 位开始截取长度为 m=N=2048 的二进制序列。然后，根据随机选择的 320 种不完全相同的编码规则 II（R_3）得到对应的 DNA 密钥序列，添加前后引物后即为密钥本。表 4 为该一次一密密钥本的一部分密钥序列。

密钥本制作好之后，根据引物对选择相应的密钥序列，对每段明文按照 DNA 碱基运算规则操作即可得到密文图像。

表 4 部分密码本

编号	密钥序列
1	ATCGCGTACG AGGCTGACTGACAGGCTGACTGACTGACTGACTGACTGACGACCTGACTGACTGAC... TTAAGCCTGT
2	TCGAACGTGGAGGCCCTTAGGCCCTTCCTTAGGCAGGCAGGCCCTTAGGCAGGCAGGCAGGCAGGC... GGATCGTAGA
3	TGCGATGCAC TCGCTCGCTCGCTCGCTCGCTCGCCCATCCATTCGCTCGCCCATCCATTCGCTCGC... GGATCGATGT
4	CGCGCGCTATAGAAAGAAAGAATGACAGAATGACTGACTGACTGACTGACAGAATGACAGAAAGAA... TGATAGCATG
5	TTAAGAGATGTTTACTATCTATCTATCTATTTTATTTATTTATTTATTTATTTCTTTCTTTCTTTCT... GACATGTCGA
6	TAGATAGTCCTTTGTTTGATACATACTTTGATACATACTTTGATACATACTTTGTTTGATACTTTG... GGTATCGCCC
7	AAACCTGGGAGCGAACCGACCGACCGGCGAGCGAGCGAGCGAGCGAGCGAACCGACCGACCGTCGG... GATGATAGTT
8	GTGTGACGAG TTAATTAAGACGTTAATTAATTAATTAAGGACGGACGGACGGACGGACTTAAGGAC... ATGCGCTAAG
9	GGGTTCGAAATTCATTCATTCAGTCAGTCATTCATTCATTCACTAGCTAGTTCATTCATTCATTCA... TTGGCGATCG
10	TAGCTGTGATGGGAGGGAGGGAGGGATGTTTGTTTGTTGGGAGGGAGACTGACTGGGAGGGAGGGA... CCCGGAGAGT

表 5 加密过程数据处理

a) Lena 图像中部分像素二进制矩阵

0000 1011	0011 0011	0111 1001
0000 1000	0011 0000	0111 1000
0000 1010	0001 1100	0110 1010
0000 1100	0001 1101	0110 1000

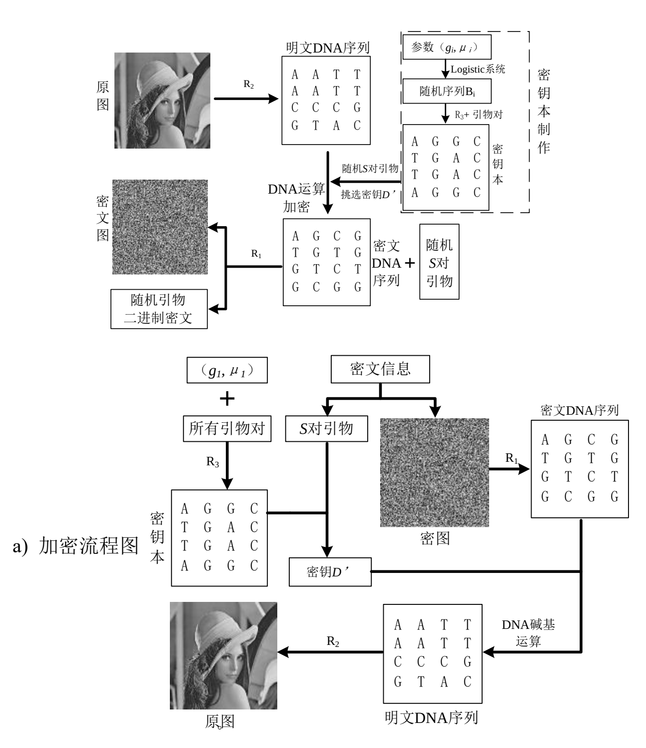
b) 明文二进制对应 DNA 序列

第一行二进制数	对应 DNA 序列
00001011 00110011 01111001	AATTAATTCCCGGTACAATTGTACA ATTGTACCCCGGTACCTTTCCCG

c) 第一行密钥分配和计算后的密文结果

引物序列	密钥序列	DNA 密文序列	对应密文二进制数
			0011101101110111
	AGGCTGACTGACAG	AGCGTGTGGTCT	1101100111101111
ATCGCGTACG-	GCTGACTGACTGACT	GCGGTGTGCCAA	0111011110100000
TTAAGCCTGT	GACTGACTGACGAC	AGTGCCAAGTCT	0011011110100000
	CTGACTGACTGAC	CCAATTGGGTCT	1101100110100000
			0101111111011001

表 5 中,a)图为原始 Lena 图像转化得到的部分二进制序列，以 a)中第一行明文为例，与密钥本中对应的加密钥进行加密操作，数据处理结果如表 5 b)和 c)所示。图像加解密的具体操作流程如图 1 所示，加密前后图像对比如图 2 所示。



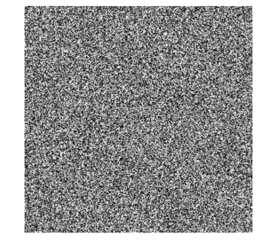
a) 加密流程图

b) 解密流程图

图 1 加解密流程图



a)Lean 原图



b)加密后图像

图 2 原图和密文图

5 算法分析

5.1 密钥空间分析

密钥空间大小和算法抵抗穷举攻击能力的大小密切相关，密钥空间越大，算法抵抗穷举攻击能力越大。本文密钥空间参数有以下几种：

a）密文二进制到 DNA 的转化对应关系为编码规则 I，不考虑互补性，R_l的选择有 N_1 种，则

$$N_1 = 24 \tag{6}$$

b）明文转换规则 R_2 选自编码规则 II，设有 N_2 种：

$$N_2 = 4^4 = 256 \tag{7}$$

c）密码本的制作也运用编码规则 II，与对明文的转化不同的是：二进制双比特可随机选择相同的四个碱基组合，即每个二进制双比特对应碱基组合的映射均有 256 种。R_3 的选择有 N_3 种，则

$$N_3 = C_{256^4}^{K} \tag{8}$$

（4）第四个步骤中，假设引物的选择有 N_4 种，则

$$N_4 = C_{4^{10}}^{2K} \tag{9}$$

其次，本文利用 Logistic 混沌映射系统生成随机数序列。此过程需要 K 对 (g_i, μ_i) 作为密钥参数,相当于存在 K 个密钥。将计算精度设置为 10^{-14}，则参数对应密钥空间的大小为 $10^{14\times K}$，K 值取决于明文分段的个数 S。

第 4 节仿真实验中 $K = 320$，综上，总的密钥空间为

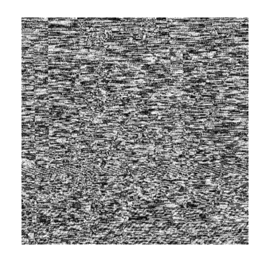
$$N_1 \times N_2 \times N_3 \times N_4 \times 10^{14\times K} = 3\times 2^{11} \times C_{256^4}^{256} \times C_{4^{10}}^{512} \times 10^{14\times 320} \tag{10}$$

显然，该算法密钥足够大，可以抵抗穷举攻击。

5.2 密钥敏感度分析

Logistic 混沌映射对系统参数十分敏感。在攻击者破译密钥本时，初始值即使有轻微的变化，解密出来的图像和原始图像就会有很大差距。以上述生成密钥本中的初始参数 $g_1 = 0.504, \mu_1 = 3.68$ 为例，若变为 $g_1 = 0.5040000000001, \mu_1 = 3.680000000001$，从同样的位置截取二进制数，通过转换得到的 DNA 序列为 AGGCTGACTGACTGACTGACAGGCTGACAGGCTGACTGACTGACTGACAGGCAGGC。

如图 3 所示，（a）是根据轻微变化所得密钥解密的图像，与（b）原始明文图像是完全不同的。



（a）错误密钥解密后图像

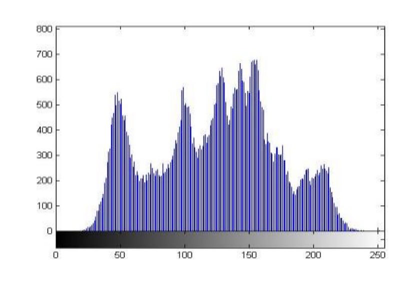


（b）正确密钥解密后图像

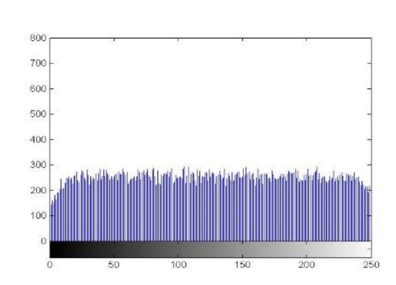
图 3 解密结果图

5.3 防统计攻击分析

灰度直方图是对图像中不同种类灰度的像素计数，是图像最基本的统计图。图 4 为原始图像加密前后的灰度直方图，可看出加密后的灰度值分布更均匀，和原图的直方图存在较大差异。因此，攻击者在密文图像中得不到任何有用的统计数据，这表明本文算法可以有效抵御使用数据的统计攻击。



a)原始图像直方图



b)密文图像直方图

图 4 直方图比较

5.4 信息熵分析

所谓信息熵，是一个度量信息量的概念。信息熵的值越高，表示一个信息越混乱，也可代表信息的不确定性更大。图像信息熵的计算公式如下：

$$H(x) = -\sum_{i=1}^{2N-1} p(x_i)\log_2 p(x_i) \tag{11}$$

研究表明，密文图像的信息熵值 $H(x)$ 越近于 8，其灰度直方图的分布越均匀，表示加密效果更强。按照以上公式计算得到本文方案的 $H(x) = 7.9433$，可见该算法对图像加密十分有效。

5.5 效率分析

根据仿真实验设定的参数，在 2.30 GHz 处理器、4 GB 内存的 PC 机上对算法进行了运行测试，分别设定了三组不同大小的灰度图像作为测试对象，每组图像均进行了 10 轮实验测试，并对 10 轮测试的加解密执行时间进行了平均值计算。算法测试结果如表 6 所示。测试结果表明，对同一大小的数据加解

密所耗费的时间基本相当，且随着数据量的增加，加解密所需耗费的时间也逐渐递增，但对三组不同大小图像的加解密时间均较短，在较为合理的范围内。

表 6 算法测试结果

图像大小	加密/s	解密/s
64*64 (5,613 Byte)	0.3526914	0.3094166
128*128 (19,277 Byte)	0.3682398	0.3616362
256*256 (66,614 Byte)	0.4473368	0.5925266

6 结束语

本文提出了一种基于 DNA 密码的加解密算法，该算法具有以下几个特点：a)对原始数据的处理所设计的 DNA 编码规则种类增加;b)加密时对明文分段操作，每一段明文数据可根据随机引物对选择不同的密钥运算，即使获得密钥本，也无法降低破解密文的难度;c)密钥本的制作以 Logistic 混沌逻辑映射为基础，满足生成序列的随机性，密钥本二进制到 DNA 序列的转换利用多碱基映射编码规则，双重保证安全性，且每次加解密使用的密钥本根据共享参数的变化而不同，可抵抗重放攻击;d)算法安全性不依赖算法本身的 DNA 运算操作，而是基于密钥本的制作规则，除了参数的获得外，还需要破解 DNA 编码的映射规则;e)该算法的密钥空间随着明文数据量的增加而增大。

参考文献：

[1] 陈霄. DNA 遗传算法及应用研究 [D]. 杭州：浙江大学, 2010. (Chen Xiao. DNA genetic algorithm and its application research [D]. Hangzhou: Zhejiang University, 2010.)

[2] Liu Qiuming, Wang Liman, Anthony G F, *et al.* DNA computing on surfaces [J]. Nature, 2000, 403 (6766): 175-9.

[3] 高琳，许进，张军英. DNA 计算的研究进展与展望 [J]. 电子学报, 2001, 29 (7): 973-977. (Gao Lin, Xu Jin, Zhang Junying. Research progress and Prospect of DNA computing [J]. Acta Electronica Sinica, 2001, 29 (7): 973-977.)

[4] 张成，杨静，王淑栋. DNA 计算中荧光技术的应用及其发展 [J]. 计算机学报, 2009, 32 (12): 2300-2310. (Zhang Cheng, Yang Jing, Wang Shudong. Application and development of fluorescence technology in DNA computing [J]. Chinese Journal of Computers, 2009, 32 (12): 2300-2310.)

[5] 李一凡，吴燃峰，杨静，等. 基于 DNA 核酶的分子加密系统 [J]. 信息网络安全, 2017 (6): 43-48. (Li Yifan, Wu Ranfeng, Yang Jing, *et al.* A molecular encryption system based on DNAzyme [J]. Netinfo Security, 2017 (6): 43-48.)

[6] Adleman L M. Molecular computation of solutions to combinatorial problems [J]. Science New, 1994, 266 (5187): 1021.

[7] Zhou Shihua, Wang Bin, Zheng Xuedong, *et al.* An image encryption scheme based on DNA computing and cellular automata [J]. Discrete Dynamics in Nature and Society, 2016, 2016 (2): 1-9.

[8] Agrawal A, Bhopale A, Sharma J, *et al.* Implementation of DNA algorithm for secure voice communication [J]. International Journal of Scientific & Engineering Research. 2012, 3 (6): 1-5.

[9] 王子成，赵晓航，王宏，等. 基于 DNA 密码的一次一密加密算法 [J]. 计算机工程与应用, 2014, 50 (15): 97-100. (Wang Zicheng, Zhao Xiaohang, Wang Hong, *et al.* One-time-pad encryption algorithm based on DNA cryptography [J]. Computer Engineering and Applications, 2014, 50 (15): 97-100.)

[10] 魏广政，金鑫，赵耿，等. 一种改进的基于 DNA 编码和混沌映射的图像加密方法 [J]. 计算机应用研究, 2015, 32 (10): 3049-3051. (Wei Guangzheng, Jin Xin, Zhao Geng, *et al.* An improved image encryption method based on DNA coding and chaotic mapping [J]. Application Research of Computer, 2015, 32 (10): 3049-3051.)

[11] Zhang Qiang, Guo Ling, Wei Xiaopeng. Image encryption using DNA addition combining with chaotic maps [J]. Mathematical and Computer Modelling, 2010, 52 (11-12): 2028-2035.

[12] Bonny B R, Vijay J F, Mahalakshmi T. Secure data transfer through DNA cryptography using symmetric algorithm [J]. International Journal of Computer Applications, 2016, 133 (2): 19-23.

[13] 陈惟昌，陈志华，陈志义，等. 遗传密码和 DNA 序列的高维空间数字编码 [J]. 生物物理学报, 2000, 16 (4): 760-768. (Chen Weichang, Chen Zhihua, Chen Zhiyi, *et al.* High dimensional spatial digital coding of genetic code and DNA sequence [J]. Acta Biophysica Sinica, 2000, 16 (4): 760-768.)